MISSOURI DEPARTMENT OF MENTAL HEALTH

Dorn Schuffman, Department Director

DEPARTMENT OPERATING REGULATION NUMBER
DOR 8.300

CHAPTER	SUBCHAPTER	EFFECTIVE DATE	NUMBER OF PAGES	PAGE NUMBER
Regulatory Compliance	HIPAA Regulations	Sept. 1, 2003	5	1 of 5

SUBJECT	AUTHORITY	History
User Access to Electronic Data	630.050	See below

PERSON RESPONSIBLE	
Director of Information Systems	Sunset Date July 1, 2007

Purpose: The policy of the Missouri Department of Mental Health is to secure consumer's protected health information in compliance with federal law and federal regulations at 45 CFR Sections164(c)(1) and (2), and 42 CFR Part 2. The practice of the Missouri Department of Mental Health is to ensure that its workforce recognizes the importance of such security provisions, and affirmatively acknowledge those guidelines.

Application: Applies to entire Department of Mental Health, its facilities and workforce.

(1) Contents

- (A) Definitions
- (B) General
- (C) User Access to DMH Data
- (D) Training on Access
- (E) Required Confidentiality Agreement
- (F) Password Management
- (G) Local Security Officer Responsibility for Local Facility Systems
- (H) DOR control
- (I) Sanctions

(2) Definitions

(A) Computer Systems – Computers connected to local and statewide communication networks, database storage or electronic records systems, Internet or email or other DMH computing devices such as PDA's or stand-alone PC's.

(B) DMH Network – Electronic network allowing access to the DMH's personal computers, facility-based systems, and centrally-based systems (e.g. mainframe, server, desktop, etc.) and electronic data.

(C) Local Area Network – Electronic network access allowing access to an individual facility's electronic data and computers.

(D) Network attached computer – Any computer with access to a local area network and/or the DMH network.

(E) DMH Workforce – Includes employees, volunteers, contract workers, trainees and other persons who are in a DMH facility or Central Office on a regular course of business. This shall include client workers employed by the DMH or any of its facilities.

(F) Consumer - Any individual who has received or is receiving services from a facility operated, licensed, certified or funded by the department of mental health.

(G) Restricted Access – Computer systems with access limited to specific systems, activities, or files.

(H) Client Work Program – any number of DMH programs which employ consumers of the Department.

(I) Confidentiality Agreement – Agreement between any business partner with which DMH shares client data which sets forth confidentiality requirements and limitations necessary for working with client, facility, and the DMH's information.

(J) Chief Security Officer (Chief Security Officer) - Individual designated by the DMH to oversee all activities related to the development, implementation, maintenance of, and adherence to Department and facility policies and procedures covering the electronic and physical security of, and access to, protected health information and other DMH data in compliance with federal and state laws and regulations.

(K) Local Security Officer (LSO) – Individual designated by a facility CEO to oversee facility information and physical security practice and policy compliance and to coordinate those activities with the Chief Security Officer.

(L) Media – Backup tapes, hard drives, floppy diskettes, CDs, zip drives cartridges, optical, and paper hard copies, etc.

(M) Protected Health Information (PHI) – Individually identifiable health information.

(3) General:

(A) Management's Right to Access Information

1. Pursuant to the Electronic Communications Privacy Act of 1986 (18 USC 2510 et seq), the department has complete access to all email and Internet activities. No electronic communications sent or received are considered private to the employee. The department has the right to monitor messages and Internet use as necessary to ensure efficient and appropriate use of the technology.

2. Each of the electronic communications technologies may create electronic records that are easily saved, copied, forwarded, retrieved, monitored, reviewed, and used for litigation. All electronic records are the property of the DMH and can be accessed and used by management when:

a. A legitimate business need exists that cannot be satisfied by other means; or

b. The involved employee is unavailable and timing is critical to a business activity; or

c. There is reasonable cause to suspect criminal activity or policy violations, or other misuse; or

d. Law, regulation, or third-party agreement requires such monitoring.

3. These disclosures of electronic records may be made without prior notice to the staff members who sent or received the communications. Staff members should not assume that any electronic communications are private.

(4) User Access to Electronic DMH Data

(A)To gain access to any DMH electronic data, DMH workforce members are required to complete the DMH Staff Access Request Form and/or the Office of Administration forms Agency Security Request (MO 300-0241N), Employee Information System On-Line Security Authorization (MO 300-0597), Sam II HR Agency Security Request (MO 300-1782N), SAM II Financial Security Request (MO 300-1765N) as appropriate. Such access shall be limited to the minimum necessary amount of protected health information to accomplish the purpose of any requested use or disclosure of PHI.

1. The appropriate supervisor or manager must approve the request(s) in writing.

2. The request form(s) must be submitted each time a user's access status changes or a user leaves the Department.

3. Users will be assigned a unique userID by the local IT staff or the Central Office Security Access Group.

4. User IDs will be password protected.

5. Network passwords will expire every 90 days.

6. Original user access forms shall be kept indefinitely in the appropriate HR file.

(B) Users shall be required to protect confidential data pursuant to DOR 8.040, Access to Consumer Protected Health Information by DMH Staff, Volunteers or Students.

(C) The CO DMH and all facilities shall maintain a Business Continuity/Disaster Recovery Plan, approved by the Chief Security Officer to ensure continued operations in the event of an emergency.

(D) No DMH consumer, volunteer, or student shall have access to another person's PHI, any DMH client demographic system, or be allowed to input information to local systems that may be used to feed or modify those systems unless they are part of the DMH workforce or are employed under the Client Work Program defined in this policy, or have data entry as part of their volunteer or student duties and responsibilities, and have signed the confidentiality statement, or unless authorized by the consumer. Any proposed consumer access shall include documentation of the consumer reviewing and agreeing to a confidentiality statement. Documentation shall include: the types of systems and files accessed.

(E) Such consumer access shall be approved by the facility director, or designee with notification and documentation provided to the Chief Security Officer.

(5) Access to Electronic Media – Internet and Electronic Mail

(A) Users are required to abide by the following guidelines when using Department electronic mail systems.

1. The Internet and email are intended to be used primarily for business purposes.

2. The Internet may be used to access external databases and files to obtain reference information or to conduct research.

3. Email may be used to disseminate business-related newsletters, press releases, or other documents to groups of people.

4. Email and the Internet may be used for discussion groups on job-related topics.

5. Personal use of email must be limited and must not interfere with the performance of work duties.

(B) Electronic mail and/or the Internet may not be used for:

1. Any illegal or unethical purpose;

2. Private purposes such as advertising products or services, business transactions, or for private business activities;

3. Operating a business, sending chain letters, or soliciting money for any purpose except for employee relations committee activities, coworker retirements or other milestone events, or events sanctioned by the Office of Administration such as blood drives or charitable campaign;

4. Transmitting, downloading or viewing material that is obscene, pornographic, threatening or harassing, or information that may reasonably be perceived to be obscene, threatening or harassing to another individual;

5. Disseminating, copying, or printing copyrighted materials (including articles, software, music and movies) in violation of copyright laws;

6. Subscribing to mailing lists and broadcast services that do not relate to the business of the Department;

7. Downloading software of any kind without prior approval of OIS;

8. Participating in Internet chat rooms or instant messaging, including but not limited to AOL Instant Messenger and Internet Relay Chat (IRC), except as authorized by the CSO and the director of the Office of Information Systems;

9. Playing games;

10. Conducting any political activity; or

11. Conducting any religious activities that are not directly business related (e.g. chaplains doing research on the Internet).

(6) Training on Access. All DMH employees, consumers, volunteers and students must receive the privacy training required by DOR 8.090.

(7) Required Confidentiality Agreement

(A) Department of Mental Health workforce members that receive or maintain PHI shall be required to agree to the security of such PHI in accordance with the state and federal laws as set forth above. These workforce members shall sign a confidentiality statement pursuant to DOR 8.040. A copy of the signed confidentiality statement shall be maintained in the personnel file of DMH staff.

(8) Password Management

(A) Passwords shall:

1. Not contain the user account number (user ID); and
2. Contain no less than 7 characters (no maximum), and
3. Contain three of the four following elements:
   a. English upper case characters (A..Z);
   b. English lower case characters (a..z);
   c. Base 10 digits (0..9);
   d. Non-alphanumeric (For example, !,$#,%).

(B) Passwords should:

1. Be changed immediately if user is aware that someone else knows it.
2. Not be entered or changed when others may see them.
3. Have no obvious connection to the user. i.e. user name, children's name, etc.; and
4. Changed completely when it expires with no easily discernable pattern.

(9) LSO's shall be responsible for auditing, monitoring, and maintaining adherence to this DOR as it applies to any and all local systems that contain PHI that is located in their facility

(10) There shall be no facility policies pertaining to this topic. The Department Operating Regulations shall control.

(11) Sanctions. Failure of workforce members to comply or ensure compliance with the DOR may result in disciplinary action, up to and including dismissal.

(12) Review Process. The Chief Security Officer will collect information from the Local Security Officers during the month of April each year beginning in 2004 for the purpose of providing feedback to the Director, Office of Information Systems and to the DMH Executive Team regarding trends and issues associated with compliance with this regulation.

History: Emergency DOR effective January 15, 2003. Final DOR effective September 1, 2003.